OWASP TOP 10

INTERNET OF THINGS 2018

1 **Weak, Guessable, or Hardcoded Passwords**

Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 **Insecure Network Services**

Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 **Insecure Ecosystem Interfaces**

Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 **Lack of Secure Update Mechanism**

Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, lack of notifications of security changes due to updates.

5 **Use of Insecure or Outdated Components**

Use of deprecated and insecure software components/libraries that could allow the device to be compromised. Including insecure customization of operating systems, and the use of third-party software or hardware components from a compromised supply chain.

6 **Insufficient Privacy Protection**

User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7 **Insecure Data Transfer and Storage**

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8 **Lack of Device Management**

Lack of security support on existing devices deployed in production, including asset management, update management, and secure decommissioning.

9 **Insecure Default Settings**

Devices or systems that are shipped with insecure default settings or lack the capability to make the system more secure.

10 **Lack of Physical Hardening**

Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

PHILOSOPHY

The OWASP Internet of Things Project was started in 2014 as a way help Developers, Manufacturers, Enterprises, and Consumers to make better decisions regarding the creation and use of IoT systems.

This continues today with the 2018 release of the OWASP IoT Top 10, which represents the top ten things to avoid when building, deploying, or managing IoT systems. The primary theme for the 2018 OWASP Internet of Things Top 10 is simplicity. Rather than having separate lists for risks vs. threats vs. vulnerabilities—or for developers vs. enterprises vs. consumers—the project team elected to have a single, unified list that captures the top things to avoid when dealing with IoT Security.

The team recognized that there are now dozens of organizations releasing elaborate guidance on IoT Security—all of which are designed for slightly different audiences and industry verticals. We thought the most useful resource we could create is a single list that addresses the highest priority issues for manufacturers, enterprises, and consumers at the same time.

The result is the 2018 OWASP IoT Top 10.

METHODOLOGY

The project team is a collection of volunteer professionals from within the security industry, with experience spanning multiple areas of expertise, including: manufacturers, consulting, security testers, developers, and many more.

The project was conducted in the following phases:

01 **Team Formation:** finding people who would be willing to contribute to the 2018 update, both as SMEs and as project leaders to perform various tasks within the duration of the project.

02 **Project Review**: analysis of the 2014 project to determine what's changed in the industry since that release, and how the list should be updated given those changes.

03 **Data Collection:** collection and review of multiple vulnerability sources (both public and private), with special emphasis on which issues caused the most actual impact and damage.

04 **Sister Project Review:** a review of dozens of other IoT Security projects to ensure that we'd not missed something major and that we were comfortable with both the content and prioritization of our release. Examples included: CSA IoT Controls Matrix, CTIA, Stanford's Secure Internet of Things Project, NISTIR 8200, ENISA IoT Baseline Report, Code of Practice for Consumer IoT Security, and others.

05 **Community Draft Feedback:** release of the draft to the community for review, including multiple Twitter calls for comments, the use of a public feedback form, and a number of public talks where feedback was gathered. The feedback was then reviewed by the team along with initial Data Collection, as well as Sister Project Review, to create the list contents and prioritization.

06 **Release:** release of the project to the public in December 2018.

THE FUTURE of the OWASP IoT Top 10

The team has a number of activities planned to continue improving on the project going forward.
Some of the items being discussed include:

- Continuing to improve the list on a two-year cadence, incorporating feedback from the community and from additional project contributors to ensure we are staying current with issues facing the industry.

- Mapping the list items to other OWASP projects, such as the ASVS, and perhaps to other projects outside OWASP as well.

- Expanding the project into other aspects of IoT—including embedded security, ICS/SCADA,etc.

- Adding use and abuse cases, with multiple examples, to solidify each concept discussed.

- Considering the addition of reference architectures, so we can not only tell people what to avoid, but how to do what they need to do securely.

Participation in the OWASP IoT Project is open to the community. We take input from all participants — whether you're a developer, a manufacturer, a penetration tester, or someone just trying to implement IoT securely. You can find the team meeting every other Friday in the the #iot-security room of the OWASP Slack Channel.

The OWASP IoT Security Team, 2018